

(19)日本国特許庁 (JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2001-306401

(P2001-306401A)

(43)公開日 平成13年11月2日(2001.11.2)

(51) Int.C1. ⁷	識別記号	F I	マークコード [*] (参考)
G06F 12/14	320	G06F 12/14	320 A 5B017
			320 B 5B035
G06K 17/00		G06K 17/00	T 5B058
19/07		G09C 1/00	660 F 5J104
19/10		G06K 19/00	N

審査請求 未請求 請求項の数17 O.L. (全17頁) 最終頁に続く

(21)出願番号 特願2001-4730(P2001-4730)
 (22)出願日 平成13年1月12日(2001.1.12)
 (31)優先権主張番号 特願2000-6989(P2000-6989)
 (32)優先日 平成12年1月14日(2000.1.14)
 (33)優先権主張国 日本(JP)
 (31)優先権主張番号 特願2000-41317(P2000-41317)
 (32)優先日 平成12年2月18日(2000.2.18)
 (33)優先権主張国 日本(JP)

(71)出願人 000005821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (72)発明者 柴田 修
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (72)発明者 湯川 泰平
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (74)代理人 100090446
 弁理士 中島 司朗

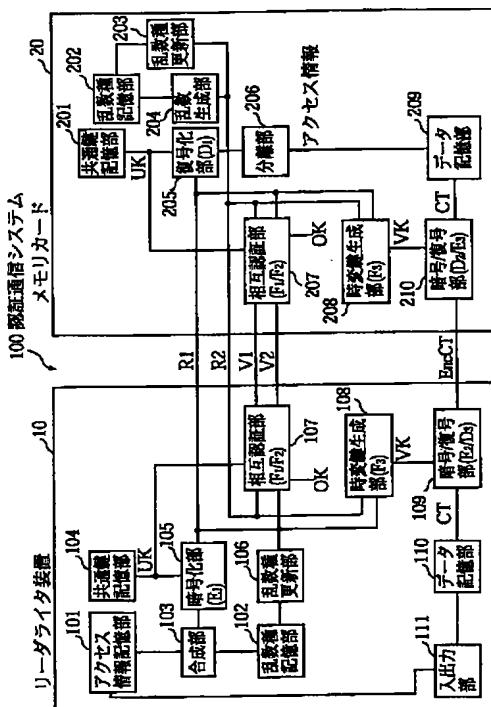
最終頁に続く

(54)【発明の名称】認証通信装置及び認証通信システム

(57)【要約】

【課題】 機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置を提供する。

【解決手段】 アクセス装置において、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を記録媒体へ伝送することにより、チャレンジレスポンス型の認証プロトコルによる記録媒体の正当性の認証を行う。記録媒体において、アクセス装置の正当性の認証を行う。記録媒体とアクセス装置とがともに正当性を有すると認証された場合に、記録媒体において、伝送された攪乱化アクセス情報からアクセス情報を分離し、アクセス装置において、分離された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む。



【特許請求の範囲】

【請求項 1】 デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであつて、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第 1 認証フェーズと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第 2 認証フェーズと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする認証通信システム。

【請求項 2】 前記第 1 認証フェーズにおいて、前記アクセス装置は、

前記領域を示すアクセス情報を取得するアクセス情報取得部と、

乱数を取得する乱数取得部と、

取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、

生成した乱数化アクセス情報に暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、

前記記録媒体は、

生成された攪乱化アクセス情報から応答値を生成する応答値生成部とを含み、

前記アクセス装置は、

生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う認証部を含むことを特徴とする請求項 1 に記載の認証通信システム。

【請求項 3】 前記転送フェーズにおいて、

前記記録媒体は、

生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化アクセス情報を生成する復号部と、

伝送された乱数化アクセス情報からアクセス情報を分離する分離部とを含むことを特徴とする請求項 2 に記載の認証通信システム。

【請求項 4】 前記第 1 認証フェーズにおいて、前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、乱数を取得することを特徴とする請求項 3 に記載の認証通信システム。

【請求項 5】 前記第 1 認証フェーズにおいて、

前記アクセス装置は、さらに、

前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きすることを特徴とする請求項 4 に記載の認証通信システム。

【請求項 6】 前記第 1 認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した乱数種に基づいて乱数を生成することに

10 より、乱数を取得することを特徴とする請求項 3 に記載の認証通信システム。

【請求項 7】 前記第 1 認証フェーズにおいて、

前記アクセス装置は、さらに、

生成された前記乱数を乱数種として前記乱数種記憶部に上書きすることを特徴とする請求項 6 に記載の認証通信システム。

【請求項 8】 前記転送フェーズにおいて、

前記領域にデジタル情報を記録している記録媒体は、

前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

前記領域からデジタル情報を読み出す前記アクセス装置は、

生成された暗号化デジタル情報を復号アルゴリズムを施してデジタル情報を生成する復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号することを特徴とする請求項 3 に記載の認証通信システム。

30 【請求項 9】 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

前記記録媒体は、

生成された前記暗号化デジタル情報を復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、

40 前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号することを特徴とする請求項 3 に記載の認証通信システム。

【請求項 10】 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

コンテンツ鍵を取得するコンテンツ鍵取得部と、

取得したコンテンツ鍵に第 1 暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第 1 暗号部と、

50 暗号化コンテンツ鍵を生成する第 1 暗号部と、

生成された前記暗号化コンテンツ鍵に第2暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第2暗号化部と、

前記コンテンツ鍵を用いて、取得した前記デジタル情報に第2暗号アルゴリズムを施して暗号化デジタル情報を生成する第3暗号部とを含み、

前記記録媒体は、

生成された前記二重暗号化コンテンツ鍵に第1復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、

前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含むことを特徴とする請求項3に記載の認証通信システム。

【請求項11】 デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムで用いられる認証通信方法であって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする認証通信方法。

【請求項12】 デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記認証通信プログラムは、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有

すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする記録媒体。

【請求項13】 請求項1に記載の認証通信システムを構成するアクセス装置。

【請求項14】 請求項2に記載の認証通信システムを構成するアクセス装置。

【請求項15】 請求項1に記載の認証通信システムを構成する記録媒体。

【請求項16】 請求項3に記載の認証通信システムを構成する記録媒体。

【請求項17】 デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムであって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする認証通信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル著作物を機器と記録媒体との間で転送する場合において、機器と記録媒体との間で、相互に正当性を認証する技術に関する。

【0002】

【従来の技術】 近年、デジタル情報圧縮技術の進展と、インターネットに代表されるグローバルな通信インフラの爆発的な普及によって、音楽、画像、映像、ゲームなどの著作物をデジタル著作物として通信回線を介して各家庭に配信することが実現されている。

【0003】 デジタル著作物の著作権者の権利や、流通業者の利益を保護するための流通配信システムを確立す

るため、通信の傍受、盗聴、なりすましなどによる著作物の不正な入手や、受信したデータを記録している記録媒体からの違法な複製、違法な改竄などの不正行為を防止することが課題となっており、正規のシステムかどうかの判別を行ったり、データスクランブルを行う暗号及び認証などの著作物保護技術が必要とされている。

【0004】著作物保護技術については、従来より様々なものが知られており、代表的なものとして、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換を行って、相互に正当性を認証しあい、正当である場合のみ、アクセスを許可するチャレンジレスポンス型の相互認証技術がある。

【0005】

【発明が解決しようとする課題】しかしながら、例えば、相互認証を正規な機器を用いて行った後に、正当機器になりすまして、機密データ記憶領域にアクセスすることにより、機密データを不正に入手する行為が考えられる。そこで本発明はかかる問題点に鑑みてなされたものであり、機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置、記録媒体、認証通信システム、認証通信方法、認証通信プログラムを記録している記録媒体及び認証通信プログラムを提供することを目的とする。

【0006】

【課題を解決するための手段】上記の目的を達成するために、本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

【0007】ここで、前記第1認証フェーズにおいて、前記アクセス装置は、前記領域を示すアクセス情報を取得するアクセス情報取得部と、乱数を取得する乱数取得部と、取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、生成した乱数化アクセス情報に暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、前記記録

媒体は、生成された攪乱化アクセス情報から応答値を生成する応答値生成部とを含み、前記アクセス装置は、生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う認証部を含むように構成してもよい。

【0008】ここで、前記転送フェーズにおいて、前記記録媒体は、生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化アクセス情報を生成する復号部と、伝送された乱数化アクセス情報からアクセス情報を分離する分離部とを含むように構成してもよい。ここ

10 で、前記第1認証フェーズにおいて、前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、乱数を取得するように構成してもよい。

【0009】ここで、前記第1認証フェーズにおいて、前記アクセス装置は、さらに、前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きするように構成してもよい。ここで、前記第1認証フェーズにおいて、前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した乱数種に基づいて乱数を生成することにより、乱数を取得するように構成してもよい。

20 20 【0010】ここで、前記第1認証フェーズにおいて、前記アクセス装置は、さらに、生成された前記乱数を乱数種として前記乱数種記憶部に上書きするように構成してもよい。ここで、前記転送フェーズにおいて、前記領域にデジタル情報を記録している記録媒体は、前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、前記領域からデジタル情報を読み出す前記アクセス装置は、生成された暗号化デジタル情報を復号アルゴリズムを施してデジタル情報を生成する復号部を含み、前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号するように構成してもよい。

30 30 【0011】ここで、前記転送フェーズにおいて、前記領域へデジタル情報を書き込む前記アクセス装置は、デジタル情報を取得するデジタル情報取得部と、取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、前記記録媒体は、生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号するように構成してもよい。

40 40 【0012】ここで、前記転送フェーズにおいて、前記領域へデジタル情報を書き込む前記アクセス装置は、デジタル情報を取得するデジタル情報取得部と、コンテン

ツ鍵を取得するコンテンツ鍵取得部と、取得したコンテンツ鍵に第1暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第1暗号部と、生成された前記暗号化コンテンツ鍵に第2暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第2暗号部と、前記コンテンツ鍵を用いて、取得した前記デジタル情報に第2暗号アルゴリズムを施して暗号化デジタル情報を生成する第3暗号部とを含み、前記記録媒体は、生成された前記二重暗号化コンテンツ鍵に第1復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含むように構成してもよい。

【0013】

【発明の実施の形態】本発明に係る一つの実施の形態としての認証通信システム100について説明する。

1. 認証通信システム100の外観と利用形態

認証通信システム100の具体的な構成例としての認証通信システム30及び31の外観図を図1(a)及び(b)に示す。

【0014】図1(a)に示すように、認証通信システム30は、パーソナルコンピュータとメモリカード20から構成される。パーソナルコンピュータは、ディスプレイ部、キーボード、スピーカ、マイクロプロセッサ、RAM、ROM、ハードディスクユニットなどを備えており、通信回線を経由してインターネットに代表されるネットワークに接続されている。メモリカード20は、メモリカード挿入口から挿入され、パーソナルコンピュータに装着される。

【0015】図1(b)に示すように、認証通信システム31は、ヘッドホンステレオ、メモリカード20及びヘッドホンから構成される。メモリカード20は、ヘッドホンステレオのメモリカード挿入口から挿入されて、ヘッドホンステレオに装着される。ヘッドホンステレオは、上面に複数の操作ボタンが配置されており、別の側面にヘッドホンが接続されている。

【0016】利用者は、メモリカード20をパーソナルコンピュータに装着し、インターネットを経由して、外部のWebサーバ装置から音楽などのデジタル著作物を取り込み、取り込んだデジタル著作物をメモリカード20に書き込む。次に、利用者は、デジタル著作物の記録されているメモリカード20をヘッドホンステレオに装着し、メモリカード20に記録されているデジタル著作物をヘッドホンステレオにより再生して、楽しむ。

【0017】ここで、パーソナルコンピュータとメモリカード20との間において、また、ヘッドホンステレオとメモリカード20との間において、チャレンジレスポンス型の認証プロトコルによる各機器の正当性の認証を行い、相互に正当な機器であることが認証された場合に

のみ、各機器間でデジタル著作物の転送が行われる。

2. 認証通信システム100の構成

認証通信システム100は、図2に示すように、リーダライタ装置10及びメモリカード20から構成される。ここで、リーダライタ装置10は、図1(a)及び(b)に示すパーソナルコンピュータ及びヘッドホンステレオに相当する。

【0018】2.1 リーダライタ装置10の構成

リーダライタ装置10は、アクセス情報記憶部101、乱数種記憶部102、合成部103、共通鍵記憶部104、暗号化部105、乱数種更新部106、相互認証部107、時変鍵生成部108、暗号復号部109、データ記憶部110及び入出力部111から構成されている。

【0019】リーダライタ装置10は、具体的には、マイクロプロセッサ、RAM、ROMその他を備え、ROMなどにコンピュータプログラムが記録されており、マイクロプロセッサは、前記コンピュータプログラムに従って動作する。

20 (1) 入出力部111

入出力部111は、利用者の操作を受け付けて、メモリカード20のデータ記憶部209に記憶されている音楽情報にアクセスするためのアクセス情報を生成する。アクセス情報は、図3に示すように、32ビット長であり、メモリカード20のデータ記憶部の領域のアドレスを示すアドレス情報と、前記領域のサイズを示すサイズ情報とから構成される。アドレス情報は、24ビット長であり、サイズ情報は、8ビット長である。

【0020】また、入出力部111は、データ記憶部110から音楽情報CTを読み出し、読み出した音楽情報CTを音声信号に変換して出力する。また、入出力部111は、利用者の操作を受け付けて、外部から音楽情報CTを取得し、取得した音楽情報CTをデータ記憶部110へ書き込む。

(2) アクセス情報記憶部101

アクセス情報記憶部101は、具体的には、半導体メモリから構成され、アクセス情報を記憶する領域を備えている。

【0021】(3) 乱数種記憶部102

乱数種記憶部102は、具体的には、半導体メモリから構成され、図3に示すような64ビット長の乱数種をあらかじめ記憶している。乱数種は、装置の製造時に記録される。乱数種記憶部102は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【0022】(4) 合成部103

合成部103は、アクセス情報記憶部101からアクセス情報を読み出し、乱数種記憶部102から乱数種を読み出す。次に、図3に示すように、読み出した前記アクセス情報と、読み出した前記乱数種の下位32ビットと

を結合して、64ビット長の乱数化アクセス情報を生成する。生成した乱数化アクセス情報を暗号化部105へ出力する。

【0023】(5) 共通鍵記憶部104

共通鍵記憶部104は、具体的には、半導体メモリから構成され、56ビット長の共通鍵UKを記憶する領域を備えている。リーダライタ装置10は、メモリカード20から共通鍵記憶部201に記憶されている共通鍵UKを秘密に取得し、共通鍵記憶部104は、取得した共通鍵UKを記憶する。

【0024】共通鍵記憶部104は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(6) 暗号化部105

暗号化部105は、共通鍵記憶部104から共通鍵UKを読み出し、合成部103から乱数化アクセス情報を受け取る。次に、暗号化部105は、共通鍵UKを用いて、受け取った乱数化アクセス情報に暗号アルゴリズムE1を施して暗号化アクセス情報R1を生成する。ここで、暗号化部105は、暗号アルゴリズムE1として、

$$(式1) \quad V2' = F1(R1, UK)$$

ここで、関数F1(a, b)は、一例として、aとbとを結合し、その結合結果に対してSHA(Secure Hash Algorithm)を施す関数である。なお、+は、結合を示す演算子である。

【0027】相互認証部107は、相互認証部207から応答値V2を受け取る。次に、相互認証部107は、V2とV2'が一致するか否かを判断し、一致しない場合には、メモリカード20が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。

$$(式2) \quad V1 = F2(R2, UK)$$

(9) 時変鍵生成部108

時変鍵生成部108は、メモリカード20が正当な装置であると認定され、動作の実行を許可される場合に、暗

$$(式3) \quad VK = F3(R1, R2)$$

次に、時変鍵生成部108は、生成した時変鍵VKを暗号復号部109へ出力する。

【0029】(10) 暗号復号部109

暗号復号部109は、時変鍵生成部108から時変鍵VKを受け取る。暗号復号部109は、暗号復号部210から暗号化音楽情報EncCTを受け取り、前記時変鍵VKを用いて、暗号化音楽情報EncCTに復号アルゴリズムD3を施して音楽情報CTを生成し、生成した音楽情報CTをデータ記憶部110へ書き込む。

【0030】ここで、暗号復号部109は、復号アルゴリズムE3として、DESを用いる。また、暗号復号部109は、データ記憶部110から音楽情報CTを読み出し、前記時変鍵VKを用いて、音楽情報CTに暗号アルゴリズムE2を施して暗号化音楽情報EncCTを生成し、生成した暗号化音楽情報EncCTを暗号復号部

DES(Data Encryption Standard)を用いる。

【0025】次に、暗号化部105は、生成した暗号化アクセス情報R1を、相互認証部107と、乱数種更新部106と、時変鍵生成部108とへ出力する。また、生成した暗号化アクセス情報R1を、メモリカード20の復号化部205と、相互認証部207と、時変鍵生成部208とへ出力する。このようにして生成された暗号化アクセス情報R1は、アクセス情報に攪乱(samble)処理を施して得られる攪乱化情報である。

【0026】(7) 乱数種更新部106

乱数種更新部106は、暗号化部105から暗号化アクセス情報R1を受け取り、受け取った暗号化アクセス情報R1を新たな乱数種として乱数種記憶部102へ上書きする。

(8) 相互認証部107

相互認証部107は、暗号化アクセス情報R1を受け取り、共通鍵記憶部104から共通鍵UKを読み出し、受け取ったR1と共に共通鍵UKとを用いて、式1により、応答値V2'を算出する。

$$= SHA(R1 + UK)$$

一致する場合には、相互認証部107は、メモリカード20が正当な装置であると認定し、他の構成部に対して以降の動作の実行を許可する。

【0028】また、相互認証部107は、乱数生成部204から乱数R2を受け取り、受け取った乱数R2と、前記共通鍵UKとを用いて、式2により、応答値V1を算出し、算出した応答値V1を相互認証部207へ出力する。

30

$$= SHA(R2 + UK)$$

号化アクセス情報R1と乱数R2とを受け取り、R1とR2とから、式3を用いて時変鍵VKを生成する

$$= SHA(R1 + R2)$$

210へ出力する。

【0031】ここで、暗号復号部109は、暗号アルゴリズムE2として、DESを用いる。

(11) データ記憶部110

40 データ記憶部110は、具体的には、半導体メモリから構成され、音楽情報CTを記憶する領域を備えている。

【0032】2.2 メモリカード20

メモリカード20は、共通鍵記憶部201、乱数種記憶部202、乱数種更新部203、乱数生成部204、復号化部205、分離部206、相互認証部207、時変鍵生成部208、データ記憶部209及び暗号復号部210から構成されている。

【0033】(1) 共通鍵記憶部201

共通鍵記憶部201は、具体的には、半導体メモリから構成され、56ビット長の共通鍵UKを記憶している。

50

共通鍵UKは、メモリカード20の製造時に記録される。共通鍵記憶部201は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【0034】(2)乱数種記憶部202

乱数種記憶部202は、具体的には、半導体メモリから構成され、64ビット長の乱数種をあらかじめ記憶している。乱数種は、メモリカード20の製造時に記録される。乱数種記憶部202は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【0035】(3)乱数生成部204

乱数生成部204は、乱数種記憶部202から乱数種を読み出し、読み出した乱数種を用いて64ビット長の乱数R2を生成し、生成した乱数R2を乱数種更新部203と、相互認証部207と、時変鍵生成部208とへ出力し、生成した乱数R2をリーダライタ装置10の相互認証部107と、時変鍵生成部108とへ出力する。

【0036】(4)乱数種更新部203

乱数種更新部203は、乱数生成部204から乱数R2を受け取り、受け取った乱数R2を新たな乱数種として乱数種記憶部202へ上書きする。

$$(式4) V2 = F1 (R1, UK) = SHA (R1 + UK)$$

ここで、F1は、式1に示すF1と同じ関数であればよい。

【0039】また、相互認証部207は、乱数生成部2

$$(式5) V1' = F2 (R2, UK) = SHA (R2 + UK)$$

ここで、F2は、式2に示すF2と同じ関数であればよい。

【0040】次に、相互認証部207は、相互認証部107からV1を受け取り、V1とV1'が一致するか否かを判断し、一致しない場合には、リーダライタ装置10が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部207は、リーダライタ装置10が正当な装置で

$$(式6) VK = F3 (R1, R2) = SHA (R1 + R2)$$

ここで、F3は、式3に示す関数F3と同じである。

【0042】次に、時変鍵生成部208は、生成した時変鍵VKを暗号復号部210へ出力する。

(9)データ記憶部209

データ記憶部209は、具体的には、半導体メモリから構成され、音楽情報CTを記憶する領域を備えている。

【0043】(10)暗号復号部210

暗号復号部210は、時変鍵生成部208から時変鍵VKを受け取る。暗号復号部210は、暗号復号部109から暗号化音楽情報EnccTを受け取り、前記時変鍵VKを用いて、暗号化音楽情報EnccTに復号アルゴリズムD2を施して音楽情報CTを生成し、生成した音楽情報CTをデータ記憶部209の前記アクセス情報により示される領域へ書き込む。

(5)復号化部205

復号化部205は、共通鍵記憶部201から共通鍵UKを読み出し、暗号化部105から暗号化アクセス情報R1を受け取る。次に、読み出した共通鍵UKを用いて、受け取った暗号化アクセス情報R1に、復号アルゴリズムD1を施して、乱数化アクセス情報を生成し、生成した乱数化アクセス情報を分離部206へ出力する。

【0037】ここで、復号化部205は、復号アルゴリズムD1として、DESを用いる。復号アルゴリズムD1は、暗号アルゴリズムE1により生成された暗号文を復号する。

(6)分離部206

分離部206は、復号化部205から乱数化アクセス情報を受け取り、受け取った乱数化アクセス情報から、その上位32ビットのデータをアクセス情報として分離し、アクセス情報をデータ記憶部209へ出力する。

【0038】(7)相互認証部207

相互認証部207は、共通鍵記憶部201から共通鍵UKを読み出し、暗号化アクセス情報R1を受け取り、受け取ったR1と共に共通鍵UKとを用いて、式4により、応答値V2を算出し、算出したV2をリーダライタ装置10の相互認証部107へ出力する。

$$(式4) V2 = F1 (R1, UK) = SHA (R1 + UK)$$

04から乱数R2を受け取り、受け取った乱数R2と、前記共通鍵UKとを用いて、式5により、応答値V1'を算出する。

$$(式5) V1' = F2 (R2, UK) = SHA (R2 + UK)$$

あると認定し、他の構成部に対して以降の動作の実行を許可する。

【0041】(8)時変鍵生成部208

時変鍵生成部208は、リーダライタ装置10が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報R1と乱数R2とを受け取り、R1とR2とから、式6を用いて時変鍵VKを生成する

$$(式6) VK = F3 (R1, R2) = SHA (R1 + R2)$$

【0044】ここで、暗号復号部210は、復号アルゴリズムD2として、DESを用いる。復号アルゴリズムD2は、暗号アルゴリズムE2により生成された暗号文を復号する。また、暗号復号部210は、データ記憶部209の前記アクセス情報により示される領域から音楽情報CTを読み出し、前記時変鍵VKを用いて、音楽情報CTに暗号アルゴリズムE3を施して暗号化音楽情報EnccTを生成し、生成した暗号化音楽情報EnccTを暗号復号部109へ出力する。

【0045】ここで、暗号復号部210は、暗号アルゴリズムE3として、DESを用いる。復号アルゴリズムD3は、暗号アルゴリズムE3により生成された暗号文を復号する。

50 3.認証通信システム100の動作

(1) 読み出し動作

認証通信システム 1 0 0 を構成するリーダライタ装置 1 0 及びメモリカード 2 0 の動作について、図 4 ~ 図 5 に示すフローチャートを用いて説明する。

【 0 0 4 6 】 なお、ここでは、リーダライタ装置 1 0 は、図 1 (b) に示すヘッドホンステレオのように、メモリカードに記憶されている情報を読み出す装置であると想定して説明する。合成部 1 0 3 は、乱数種記憶部 1 0 2 から乱数種を読み出し、アクセス情報記憶部 1 0 1 からアクセス情報を読み出し、読み出した前記乱数種と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成し (ステップ S 1 0 1) 、暗号化部は、共通鍵記憶部 1 0 4 から共通鍵を読み出し、読み出した前記共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報を R 1 を生成し (ステップ S 1 0 2) 、相互認証部 1 0 7 は、 $V_2' = F_1(R_1)$ を算出し (ステップ S 1 0 3) 、乱数種更新部 1 0 6 は、生成された乱数化アクセス情報を新たな乱数種として乱数種記憶部 1 0 2 に上書きする (ステップ S 1 0 4) 。

【 0 0 4 7 】 暗号化部 1 0 5 は、生成した暗号化アクセス情報を R 1 をメモリカード 2 0 へ出力し、メモリカードの相互認証部 2 0 7 は、暗号化アクセス情報を R 1 を受け取る (ステップ S 1 0 5) 。相互認証部 2 0 7 は、 $V_2 = F_1(R_1)$ を算出し (ステップ S 1 0 6) 、 V_2 をリーダライタ装置 1 0 の相互認証部 1 0 7 へ出力し、相互認証部 1 0 7 は、 V_2 を受け取る (ステップ S 1 0 7) 。

【 0 0 4 8 】 相互認証部 1 0 7 は、 V_2 と V_2' とが一致するか否かを判断し、一致しない場合には (ステップ S 1 0 8) 、メモリカード 2 0 が不正な装置であると認定し、以後の動作を中止する。一致する場合には (ステップ S 1 0 8) 、相互認証部 1 0 7 は、メモリカード 2 0 が正当な装置であると認定し、メモリカード 2 0 の乱数生成部 2 0 4 は、乱数種記憶部 2 0 2 から乱数種を読み出し、読み出した乱数種を用いて乱数 R 2 を生成し (ステップ S 1 0 9) 、相互認証部 2 0 7 は、 $V_1' = F_2(R_2)$ を算出し (ステップ S 1 1 0) 、乱数種更新部 2 0 3 は、生成された乱数 R 2 を新たに乱数種として乱数種記憶部 2 0 2 に上書きする (ステップ S 1 1 1) 。次に、乱数生成部 2 0 4 は、生成した乱数 R 2 をリーダライタ装置 1 0 の相互認証部 1 0 7 へ出力し、相互認証部 1 0 7 は、乱数 R 2 を受け取り (ステップ S 1 1 2) 、相互認証部 1 0 7 は、 $V_1 = F_2(R_2)$ を生成し (ステップ S 1 1 3) 、生成した V_1 をメモリカード 2 0 の相互認証部 2 0 7 へ出力し、相互認証部 2 0 7 は、 V_1 を受け取る (ステップ S 1 1 4) 。

【 0 0 4 9 】 次に、相互認証部 2 0 7 は、 V_1 と V_1' とが一致するか否かを判断し、一致しない場合には (ステップ S 1 1 5) 、リーダライタ装置 1 0 が不正な装置であると認定し、以後の動作を中止す

る。一致する場合には (ステップ S 1 1 5) 、相互認証部 2 0 7 は、リーダライタ装置 1 0 が正当な装置であると認定し、リーダライタ装置 1 0 の時変鍵生成部 1 0 8 は、R 1 と R 2 とを用いて時変鍵 VK を生成する (ステップ S 1 2 1) 。メモリカード 2 0 0 の復号化部 2 0 5 は、共通鍵記憶部 2 0 1 から共通鍵 UK を読み出し、読み出した共通鍵 UK を用いて R 1 を復号して乱数化アクセス情報を生成し (ステップ S 1 2 2) 、分離部 2 0 6 は、乱数化アクセス情報を分離し (ステップ S 1 2 3) 、時変鍵生成部 2 0 8 は、R 1 と R 2 とを用いて時変鍵 VK を生成し (ステップ S 1 2 4) 、暗号復号部 2 1 0 は、アクセス情報をにより示されるデータ記憶部 2 0 9 の領域から音楽情報 CT を読み出し (ステップ S 1 2 5) 、暗号復号部 2 1 0 は、生成された時変鍵 VK を用いて読み出した前記音楽情報 CT を暗号化して暗号化音楽情報 E n c C T を生成し (ステップ S 1 2 6) 、生成した暗号化音楽情報 E n c C T をリーダライタ装置 1 0 の暗号復号部 1 0 9 へ出力する (ステップ S 1 2 7) 。

【 0 0 5 0 】 暗号復号部 1 0 9 は、時変鍵 VK を用いて暗号化音楽情報を E n c C T を復号して音楽情報を生成してデータ記憶部 1 1 0 へ書き込み (ステップ S 1 2 8) 、入出力部 1 1 1 は、音楽情報を CT をデータ記憶部 1 1 0 から読み出し、読み出した音楽情報を CT を音声信号に変換して出力する (ステップ S 1 2 9) 。

(2) 書き込み動作

認証通信システム 1 0 0 を構成するリーダライタ装置 1 0 及びメモリカード 2 0 の動作について、図 6 に示すフローチャートを用いて説明する。

【 0 0 5 1 】 ここでは、リーダライタ装置 1 0 は、図 1 (a) に示すパーソナルコンピュータのように、メモリカードに情報を書き込む装置であると想定して説明する。また、読み出し動作と書き込み動作は類似しているので、相違点のみについて説明する。図 4 ~ 図 5 のフローチャートのステップ S 1 2 5 ~ S 1 2 9 を、図 6 に示すステップに置き換えると認証通信システム 1 0 0 の書き込み動作となる。

【 0 0 5 2 】 暗号復号部 1 0 9 は、データ記憶部 1 1 0 から音楽情報を CT を読み出し (ステップ S 1 3 1) 、時変鍵 VK を用いて読み出した音楽情報を CT を暗号化して暗号化音楽情報を CT を生成し (ステップ S 1 3 2) 、生成した暗号化音楽情報を CT をメモリカード 2 0 の暗号復号部 2 1 0 へ出力し、暗号復号部 2 1 0 は、暗号化音楽情報を CT を受け取る (ステップ S 1 3 3) 。

【 0 0 5 3 】 暗号復号部 2 1 0 は、暗号化音楽情報を E n c C T を時変鍵 VK を用いて復号して音楽情報を CT を生成し (ステップ S 1 3 4) 、生成した音楽情報を CT を前記アクセス情報を示されるデータ記憶部 2 0 9 内の領域に書き込む (ステップ S 1 3 5) 。

4. まとめ

以上説明したように、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

【0054】また、仮に機密データ記憶領域にアクセスするための情報が、不正ななりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が確立しないので、機密データ記憶領域にアクセスできないようになることができる。また、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

【0055】5. 認証通信システム100a
認証通信システム100の変形例としての認証通信システム100aについて説明する。

5. 1 認証通信システム100aの構成

認証通信システム100aは、図7に示すように、リーダライタ装置10aとメモリカード20とから構成される。

【0056】メモリカード20は、図2に示すメモリカード20と同じであるので、ここでは、説明を省略する。リーダライタ装置10aは、アクセス情報記憶部101、乱数種記憶部102、合成部103、共通鍵記憶部104、暗号化部105、乱数種更新部106、相互認証部107、時変鍵生成部108、暗号復号部109、データ記憶部110、入出力部111及び乱数生成部112から構成されている。

【0057】リーダライタ装置10との相違点を中心として、以下に説明する。その他の点については、リーダライタ装置10と同じであるので、説明を省略する。

(1) 亂数生成部112

乱数生成部112は、乱数種記憶部102から乱数種を読み出し、読み出した乱数種を用いて64ビット長の乱数を生成し、生成した乱数を合成部103と乱数種更新部106とへ出力する。

(2) 亂数種更新部106

乱数種更新部106は、乱数生成部112から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部102へ上書きする。

(3) 合成部103

合成部103は、乱数生成部112から乱数を受け取り、アクセス情報記憶部101からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成する。

【0059】5. 2 認証通信システム100aの動作
認証通信システム100aの動作について、図8に示すフローチャートを用いて説明する。乱数生成部112は、乱数種記憶部102から乱数種を読み出し（ステップS201）、読み出した乱数種を用いて64ビット長の乱数を生成し（ステップS202）、乱数種更新部1

06は、乱数生成部112から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部102へ上書きする（ステップS203）。次に、合成部103は、乱数生成部112から乱数を受け取り、アクセス情報記憶部101からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成する（ステップS204）。

【0060】次に、図4のステップS102へ続く。以下は、認証通信システム100の動作と同じであるので、説明を省略する。

5. 3 まとめ

以上説明したように、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

【0061】6. 認証通信システム100b

認証通信システム100aの変形例としての認証通信システム100bについて説明する。

6. 1 認証通信システム100bの構成

認証通信システム100bは、図9に示すように、リーダライタ装置10bとメモリカード20bとから構成される。

【0062】(1) リーダライタ装置10bの構成

リーダライタ装置10bは、アクセス情報記憶部101、乱数種記憶部102、合成部103、共通鍵記憶部104、暗号化部105、乱数種更新部106、相互認証部107、時変鍵生成部108、データ記憶部110、入出力部111、乱数生成部112、コンテンツ鍵生成部113、暗号化部114、コンテンツ付加情報記憶部115、暗号復号部116及び暗号化部117から構成されている。

【0063】以下において、リーダライタ装置10aとの相違点を中心として説明する。その他の点については、リーダライタ装置10aと同じであるので、説明を省略している。

(a) 入出力部111

入出力部111は、利用者の操作によりコンテンツ付加情報の入力を受け付け、受け付けたコンテンツ付加情報をコンテンツ付加情報記憶部115に書き込む。

【0064】ここで、コンテンツ付加情報の一例は、コンテンツの再生回数、使用期間であり、コンテンツ付加情報は、8ビット長である。また、入出力部111は、利用者の操作によりコンテンツデータCDを取得し、取得したコンテンツデータCDをデータ記憶部110に書き込む。ここで、コンテンツデータCDは、一例として音楽コンテンツ情報である。

【0065】(b) 亂数生成部112

乱数生成部112は、生成した乱数R3をコンテンツ鍵生成部113へ出力する。

(c) コンテンツ鍵生成部113

コンテンツ鍵生成部 113 は、コンテンツ付加情報記憶部 115 からコンテンツ付加情報を読み出し、乱数生成部 112 から乱数 R3 を受け取り、乱数 R3 と読み出し

$$(式 7) CK = F4 (R3, コンテンツ付加情報) \\ = コンテンツ付加情報 (8 ビット長) + R3 の下位 56 ビット$$

ここで、+ は、データとデータの結合を示す演算子である。

【0066】次に、コンテンツ鍵生成部 113 は、生成したコンテンツ鍵 CK を暗号化部 114 と、暗号化部 117 とへ出力する。

(d) 暗号化部 114

暗号化部 114 は、コンテンツ鍵生成部 113 からコンテンツ鍵 CK を受け取り、共通鍵記憶部 104 から共通鍵 UK を読み出し、読み出した共通鍵 UK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E4 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を暗号復号部 116 へ出力する。

【0067】ここで、暗号化部 114 は、暗号アルゴリズム E4 として、DES を用いる。

(e) 暗号復号部 116

暗号復号部 116 は、暗号化部 114 から暗号化コンテンツ鍵 Enc CK を受け取り、受け取った暗号化コンテンツ鍵 Enc CK に、時変鍵 VK を用いて、暗号アルゴリズム E2 を施して Enc (Enc CK) を生成し、生成した Enc (Enc CK) を暗号復号部 211 へ出力する。

【0068】ここで、暗号復号部 116 は、暗号アルゴリズム E2 として、DES を用いる。

(f) 暗号化部 117

暗号化部 117 は、データ記憶部 110 からコンテンツデータ CD を読み出し、読み出したコンテンツデータ CD に、コンテンツ鍵 CK を用いて、暗号化アルゴリズム E5 を施して暗号化コンテンツデータ Enc CD を生成する。次に、暗号化部 117 は、生成した暗号化コンテンツデータ Enc CD をデータ記憶部 213 へ出力する。

【0069】ここで、暗号化部 117 は、暗号アルゴリズム E5 として、DES を用いる。

(2) メモリカード 20b の構成

メモリカード 20b は、共通鍵記憶部 201、乱数種記憶部 202、乱数種更新部 203、乱数生成部 204、復号化部 205、分離部 206、相互認証部 207、時変鍵生成部 208、暗号復号部 211、鍵データ記憶部 212 及びデータ記憶部 213 から構成されている。

【0070】以下において、メモリカード 20 との相違点を中心として説明する。その他の点については、メモリカード 20 と同じであるので、説明を省略している。

(a) 時変鍵生成部 208

時変鍵生成部 208 は、時変鍵 VK を暗号復号部 211

たコンテンツ付加情報を用いて、式 7 により、コンテンツ鍵 CK を生成する。ここで、コンテンツ鍵 CK は、64 ビット長である。

（8 ビット長） + R3 の下位 56 ビット

へ出力する。

(b) 暗号復号部 211

暗号復号部 211 は、時変鍵生成部 208 から時変鍵 VK を受け取り、暗号復号部 116 から Enc (Enc CK) を受け取る。

【0071】次に、暗号復号部 211 は、時変鍵 VK を用いて Enc (Enc CK) に復号アルゴリズム D2 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を前記アクセス情報により示される鍵データ記憶部 212 の領域に書き込む。

(c) 鍵データ記憶部 212

鍵データ記憶部 212 は、暗号化コンテンツ鍵 Enc CK を記憶する領域を備える。

【0072】(d) データ記憶部 213

データ記憶部 213 は、暗号化コンテンツデータ Enc CD を受け取り、受け取った暗号化コンテンツデータ Enc CD を記憶する。

6. 2 認証通信システム 100b の動作

認証通信システム 100b の動作は、認証通信システム 100a の動作に類似している。ここでは、認証通信システム 100a との相違点についてのみ説明する。

【0073】認証通信システム 100b の動作は、認証通信システム 100a の動作を示すフローチャートのうち、ステップ S121 以降を図 10 に示すフローチャートに置き換えたフローチャートにより示される。コンテンツ鍵生成部 113 は、コンテンツ付加情報記憶部 115 からコンテンツ付加情報を読み出し (ステップ S301)、乱数生成部 112 は、生成した乱数 R3 をコンテンツ鍵生成部 113 へ出力し、コンテンツ鍵生成部 113 は、乱数生成部 112 から R3 を受け取り、R3 と読み出したコンテンツ付加情報を用いて、コンテンツ鍵 CK を生成し、生成したコンテンツ鍵 CK を暗号化部 114 へ出力し (ステップ S302)、暗号化部 114 は、コンテンツ鍵生成部 113 からコンテンツ鍵 CK を受け取り、共通鍵記憶部 104 から

共通鍵 UK を読み出し、読み出した共通鍵 UK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E4 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を暗号復号部 116 へ出力する (ステップ S303)。次に、暗号復号部 116 は、暗号化コンテンツ鍵 Enc CK を受け取り、受け取った暗号化コンテンツ鍵 Enc CK に時変鍵 VK を用いて暗号アルゴリズム E2 を施して Enc (Enc CK) を生成し (ステップ S304)、暗号復号部 116 は、生成した Enc (Enc CK) を暗号復号部

211へ出力し、暗号復号部211は、E n c (E n c CK)を受け取り(ステップS305)、暗号復号部211は、E n c (E n c CK)に時変鍵V Kを用いて復号アルゴリズムD2を施して暗号化コンテンツ鍵E n c CKを生成し、生成した暗号化コンテンツ鍵E n c CKを前記アクセス情報により示される鍵データ記憶部212の領域に書き込む(ステップS306)。

【0074】暗号化部117は、データ記憶部110からコンテンツデータCDを読み出し(ステップS307)、読み出したコンテンツデータCDにコンテンツ鍵CKを用いて暗号化アルゴリズムE5を施して暗号化コンテンツデータE n c C Dを生成する(ステップS308)。暗号化部117は、生成した暗号化コンテンツデータE n c C Dをデータ記憶部213へ出力し、データ記憶部213は、暗号化コンテンツデータE n c C Dを受け取り(ステップS309)、データ記憶部213は、受け取った暗号化コンテンツデータE n c C Dを記憶する(ステップS310)。

【0075】6. 3まとめ

以上説明したように、認証通信システム100bにおいて、コンテンツデータを暗号化するためのコンテンツ鍵を生成するのに、新たな乱数発生機構を必要とせず、アクセス情報の合成に用いる乱数発生機構と共有化できる。

7. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【0076】(1) 上記の実施の形態において、デジタル著作物は、音楽の情報であるとしているが、小説や論文などの文字データ、コンピュータゲーム用のコンピュータプログラムソフトウェア、MP3などに代表される圧縮された音声データ、JPEGなどの静止画像、MP EGなどの動画像であるとしてもよい。また、リーダライタ装置は、パーソナルコンピュータに限定されず、上記の様々なデジタル著作物を販売したり配布したりする出力装置であるとしてもよい。また、リーダライタ装置は、ヘッドホンステレオに限定されず、デジタル著作物を再生する再生装置であるとしてもよい。例えば、コンピュータゲーム装置、帯型情報端末、専用装置、パーソナルコンピュータなどであるとしてもよい。また、リーダライタ装置は、上記出力装置と再生装置との両方を兼ね備えているとしてもよい。

【0077】(2) 上記の実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、DESを用いるとしているが、他の暗号を用いるとしてもよい。また、上記実施の形態において、SHAを用いるとしているが、他的一方向性関数を用いるとしてもよい。共通鍵、時変鍵の鍵長は、56ビットであるとしているが、他の長さ

の鍵を用いるとしてもよい。

【0078】(3) 上記の実施の形態において、合成功能部103は、アクセス情報と、乱数種の下位32ビットとを結合して、64ビット長の乱数化アクセス情報を生成するとしているが、これに限定されない。次のようにしてもよい。合成功能部103は、32ビットのアクセス情報と、乱数種の下位32ビットとを1ビットずつ交互に結合して、64ビット長の乱数化アクセス情報を生成している。また、複数ビットずつ交互に結合してもよい。この場合、分離部206は、逆の操作を行うようとする。

【0079】(4) 上記の実施の形態において、メモリカード20の乱数生成部204は、乱数種記憶部202に記憶されている乱数種を用いて乱数R2を生成しているが、乱数生成部204は、乱数種を乱数R2として生成してもよい。また、時変鍵生成部108、208は、R1及びR2を用いて時変鍵を生成するとしているが、応答値を用いるとしてもよい。また、共通鍵UKを絡ませてもよい。

【0080】(5) 認証通信システム100bにおいて、暗号化部117は、暗号化コンテンツデータE n c C Dをデータ記憶部213に書き込むとしているが、暗号化コンテンツデータE n c C Dを機密データとして扱って、アクセス情報により示される領域に書き込むとしてもよい。また、暗号化コンテンツ鍵E n c CKを機密データとして扱わずに、データ記憶部213に書き込むとしてもよい。

【0081】また、暗号化部114及び暗号化部117のいずれか一方を無くし、残っている一方により共有化してもよい。

(6) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0082】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピー(登録商標)ディスク、ハードディスク、CD-ROM、MO、DVD、DV D-R OM、DV D-R AM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0083】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサ

は、前記コンピュータプログラムに従って動作するとしてもよい。

【0084】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(4) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0085】8. 産業上の利用の可能性

デジタル著作物を出力する出力装置から半導体記録媒体へデジタル著作物を複製する場合において、出力装置と半導体記録媒体とが、相互に正当性を認証する場合に利用することができる。また、デジタル著作物の記録されている半導体記録媒体からデジタル著作物を読み出して再生する場合において、半導体記録媒体と再生装置との間で、各装置が、相互に正当性を認証する場合に利用することができる。

【0086】

【発明の効果】上記目的を達成するために本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

【0087】これによって、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。また、仮に、機密データ記憶領域にアクセスするための情報が、不正なりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が成功しないので、機密データ記憶領域にアクセスできないようになることができる。

【図面の簡単な説明】

【図1】図1は、認証通信システム100の具体的な構成例としての認証通信システム30及び31の外観を示す。図1(a)は、パーソナルコンピュータとメモリカ

ード20から構成される認証通信システム30の外観を示し、図1(b)は、ヘッドホンステレオ、メモリカード20及びヘッドホンから構成される認証通信システム31の外観を示す。

【図2】図2は、認証通信システム100を構成するリーダライタ装置10及びメモリカード20のそれぞれ構成を示すブロック図である。

【図3】図3は、アクセス情報、乱数種及び乱数化アクセス情報のデータ構造を示す。

10 【図4】図4は、認証通信システム100の動作を示すフローチャートであり、特に、メモリカードに記憶されている情報を読み出す場合を想定したものである。図5に続く。

【図5】図5は、認証通信システム100の動作を示すフローチャートである。図4から続く。

【図6】図6は、認証通信システム100の動作を示すフローチャートであり、特に、リーダライタ装置10は、メモリカードに情報を書き込む装置であると想定した場合のものである。

【図7】図7は、別の実施の形態としての、認証通信システム100aの構成を示すブロック図である。

【図8】図8は、認証通信システム100aに固有の動作を示すフローチャートである。

【図9】図9は、別の実施の形態としての、認証通信システム100bの構成を示すブロック図である。

【図10】図10は、認証通信システム100bに固有の動作を示すフローチャートである。

【符号の説明】

100 認証通信システム

30 10 リーダライタ装置

101 アクセス情報記憶部

102 乱数種記憶部

103 合成部

104 共通鍵記憶部

105 暗号化部

106 乱数種更新部

107 相互認証部

108 時変鍵生成部

109 暗号復号部

40 110 データ記憶部

111 入出力部

20 メモリカード

201 共通鍵記憶部

202 乱数種記憶部

203 乱数種更新部

204 乱数生成部

205 復号化部

206 分離部

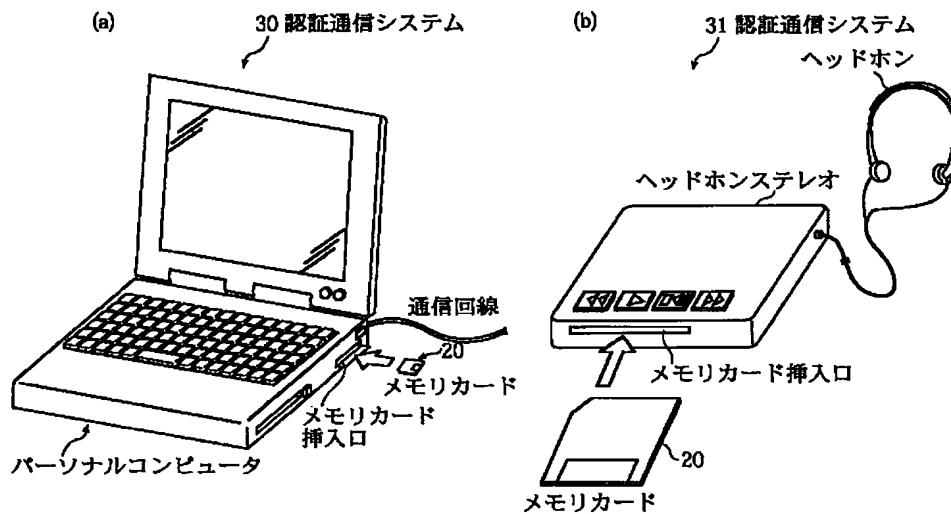
207 相互認証部

50 208 時変鍵生成部

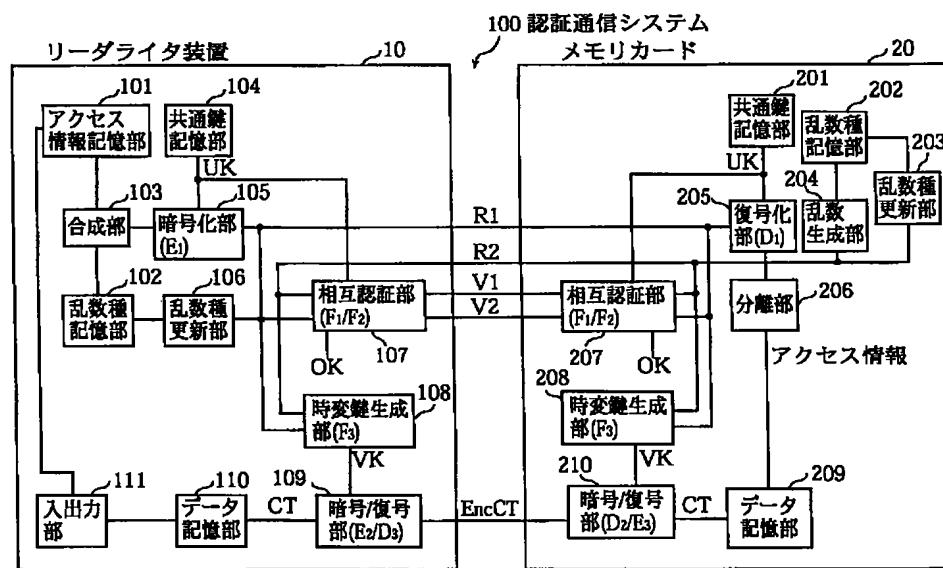
209 データ記憶部

210 暗号復号部

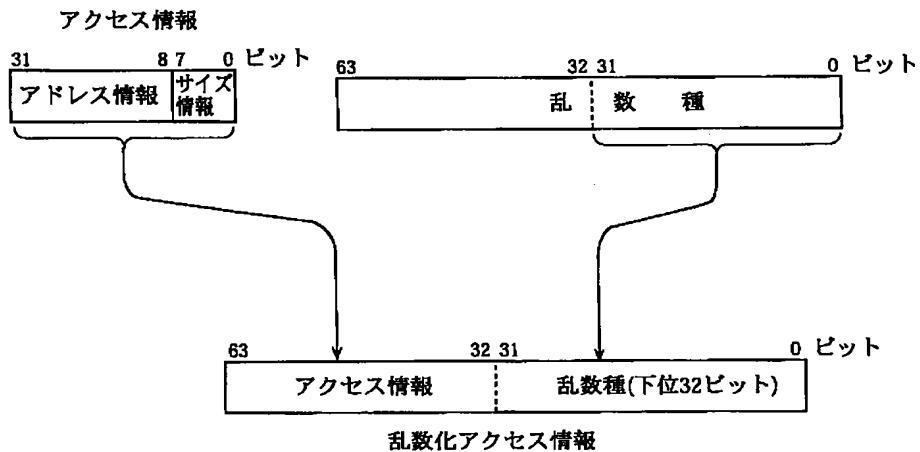
【図1】



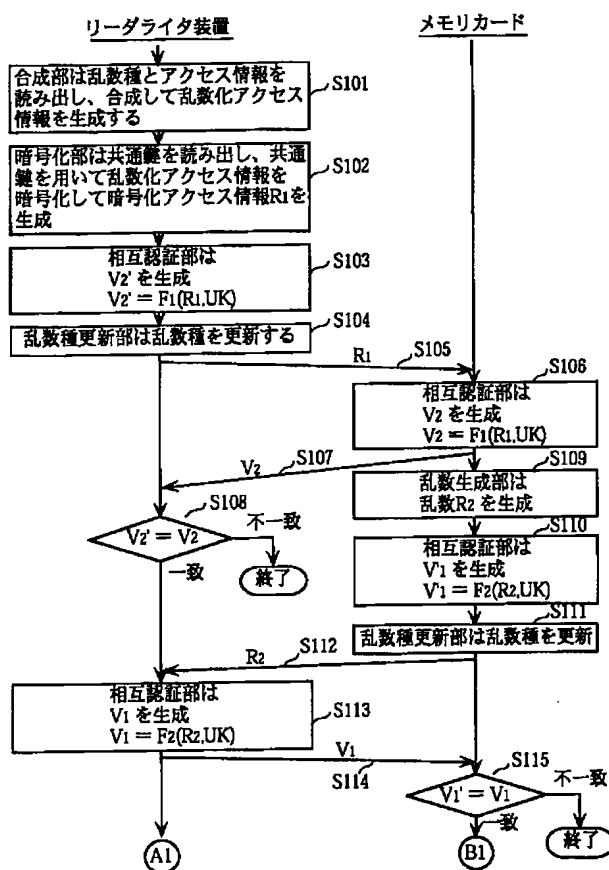
【図2】



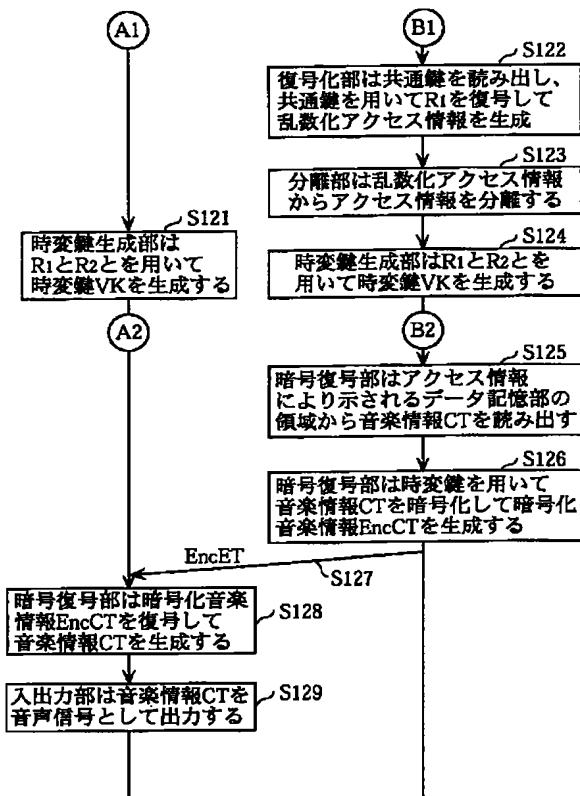
【図 3】



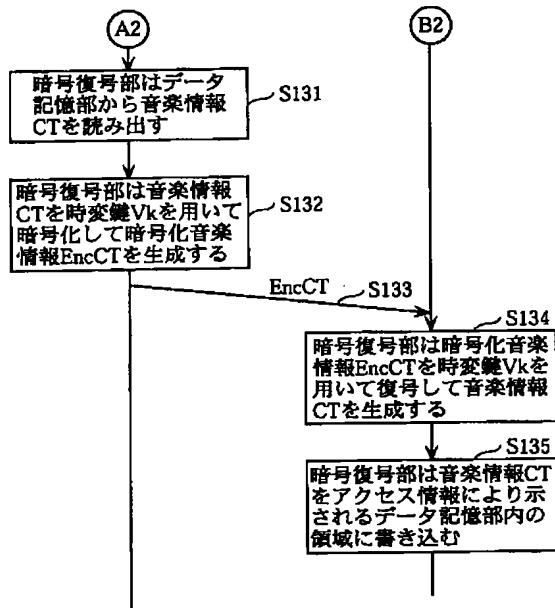
【図 4】



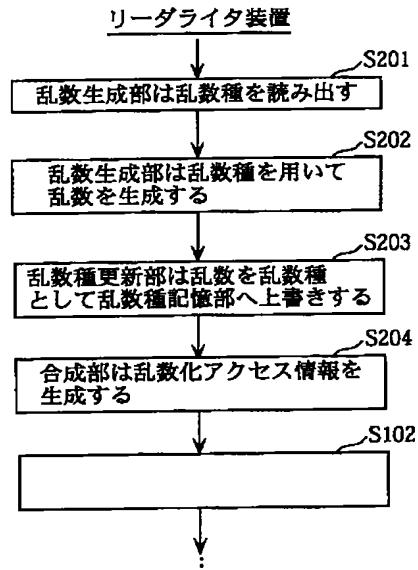
【図 5】



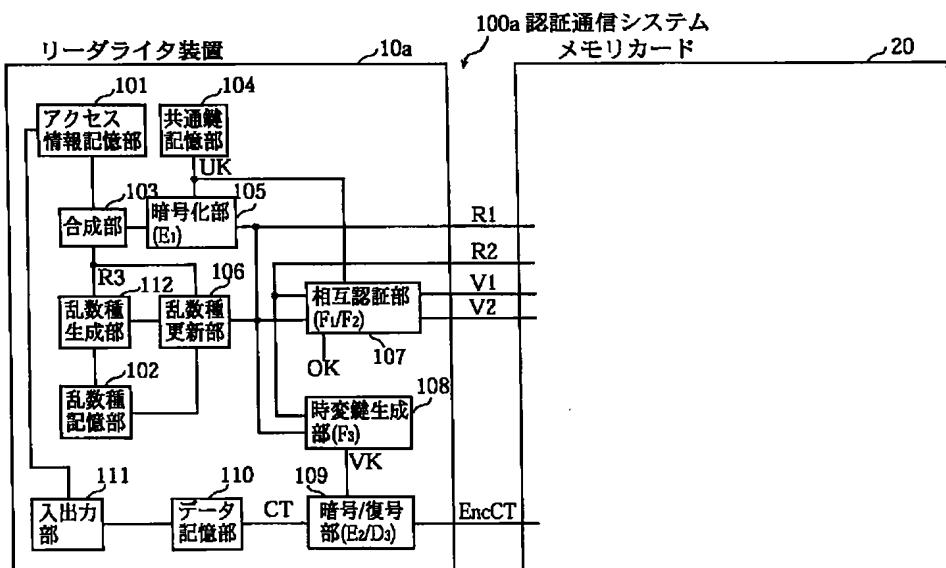
【図 6】



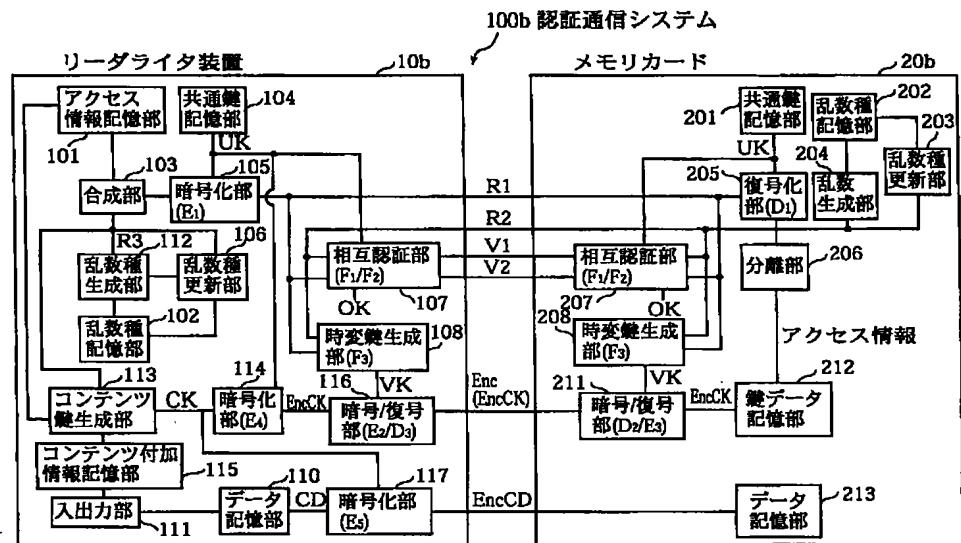
【図 8】



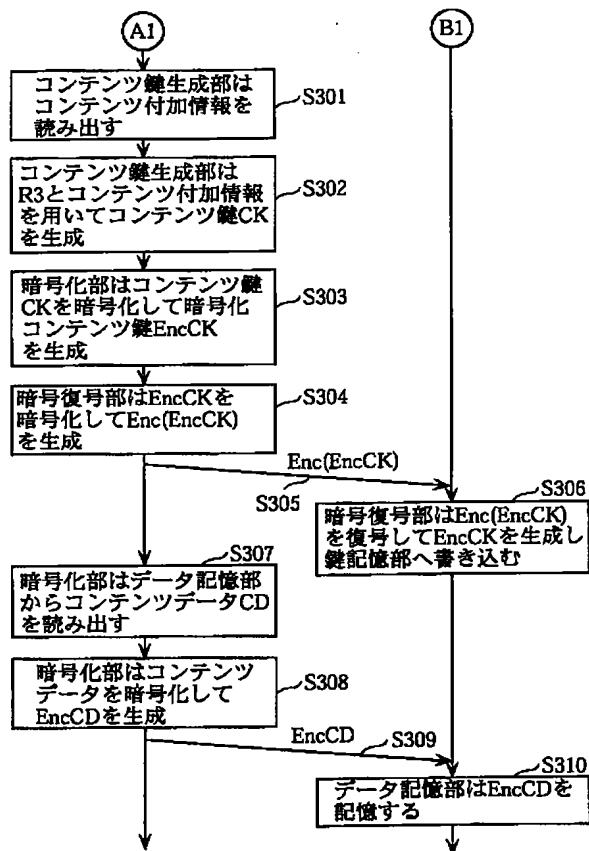
【図 7】



【図 9】



【図 10】



フロントページの続き

(51) Int.C1. ⁷	識別記号	F I	「マークコード」(参考)
G 0 9 C	1/00	G 0 6 K	19/00 R
H 0 4 L	9/08	H 0 4 L	9/00 6 0 1 A
	9/10		6 2 1 A
	9/32		6 7 5 A
(72) 発明者 関部 勉		(72) 発明者 大竹 俊彦	
大阪府門真市大字門真1006番地 松下電器		大阪府門真市大字門真1006番地 松下電器	
産業株式会社内		産業株式会社内	
(72) 発明者 廣田 照人		F ターム(参考) 5B017 AA03 BA05 BA07 CA14	
大阪府門真市大字門真1006番地 松下電器		5B035 AA13 BB09 BC00 CA11	
産業株式会社内		5B058 CA27 KA02 KA04 KA08 KA35	
(72) 発明者 齊藤 義行		YA20	
大阪府門真市大字門真1006番地 松下電器		5J104 AA01 AA07 AA15 AA16 EA06	
産業株式会社内		EA07 JA13 KA02 KA04 KA06	
		NA02 NA35 NA37	